SUBJECT: Protecting Patient Privacy under the caBIG™ Program	SOP No.: AD-005
	Version No.: 2.0
	Effective Date: 12/11/2006
	Page 1 of 7 Pages

Standard Operating Procedure – Protecting Patient Privacy under the caBIG™ Program

This cover sheet controls the layout and components of the entire document.

Issued Date: October 30, 2006

Effective Date: December 11, 2006

Department Approval:

Peter Covitz

Chief Operating Officer, NCICB

QA Approval:

George Komatsoulis

Director of Quality Assurance

Note: This document will be issued for training on the Issue Date. The document will become available for use to trained personnel on the Effective Date. Before using this document, make sure it is the latest revision. Access the caBIG™ website to verify the current revision.

Revision History

Revision	Date	Author	Change Reference	Reason for Change
1.0	09/19/2005	SOP Working Group	N/A	Initial release.
2.0	10/30/2006	BP SIG/SOP WG	All pages	Annual update.

1. Purpose

The purpose of this Standard Operating Procedure (SOP) is to describe the information privacy responsibilities of caBIG™ participants with access to systems maintained by the National Cancer Institute Center for Bioinformatics (NCICB). Fulfilling these responsibilities will ensure that institutional privacy procedures are consistent with the *Secure One HHS Information Security Program Policy* and federal legal requirements; and compatible with the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to many of the cancer centers. This Standard Operating Procedure will facilitate collaborative research efforts among cancer centers and other institutions.

2. Scope

This SOP advises all users of NCICB clinical data management systems on what minimum steps are required to assure that the privacy of patient data submitted to, and provided by, the NCICB clinical data management system applications are adequately protected. These requirements are consistent with those of the HIPAA Privacy Rule and best practices. In addition to the activities described, participating institutions should identify and implement all privacy control measures reasonable and necessary to protect the confidentiality, integrity, and availability of any information they send, receive, use, or store using NCICB clinical data management systems. Participating cancer centers and other institutions understand and accept that addressing this SOP alone will not constitute compliance with the HIPAA Privacy Rule.

3. Requirements

3.1 *Privacy policies and procedures.* All caBIG™ participants and other institutions seeking access to the caBIG™ systems maintained by NCICB must maintain comprehensive policies and procedures to prevent, detect, contain, and correct privacy violations. Centers covered under the HIPAA Privacy Rule will maintain compliance with the policies and procedures required by the Rule; and all others will assure that all reasonable and necessary privacy policies and procedures have been developed and implemented at their institutions. Policies may be incorporated into any existing information privacy policies maintained by the cancer center or other institution. Privacy policies must, at minimum, require cancer centers to:

3.1.1 Provide a privacy notice to subjects as to how their data will be used by the caBIG™ participants (*See* HIPAA Privacy Rule, 42 CFR 164.520, *Notice of privacy practices for protected health information*).

3.1.2 Identify cancer center workforce member(s) who will be responsible for enforcing privacy policies (*See* HIPAA Privacy Rule, 42 CFR 164.530 (a)(1), *Standard: Personnel designations*).

3.1.3 Restrict use and disclosure of protected health information, collected for the purposes of submission to NCICB clinical data management systems, to research purposes, provided that the documentation has been obtained of an alteration to or waiver of an individual authorization (as required by 42 CFR 164.508) has been approved by either an Institutional Review Board or

Privacy Board (*See* HIPAA Privacy Rule, 42 CFR 164.512(i), *Standard: Uses and disclosures for research purposes*).

3.2 *Common Rule compliance.* All caBIG™ participant cancer centers and other institutions seeking access to the systems supported by NCICB must maintain comprehensive policies and procedures to review research proposals involving human subjects, including the submission of patient data (whether or not in identifiable form) to these applications, consistent with the Common Rule for Review of Human Subjects Research (45 CFR 46.101 *et seq*.). Policies may be incorporated into any existing information privacy policies maintained by the cancer center or other institution. Privacy policies must require cancer centers to:

3.2.1 Obtain consent of human subjects before supplying their data to NCICB systems (45 CFR 46.109, *IRB review of research*, and 46.116, *General Requirements for informed consent*).

3.2.2 Submit all proposals for research involving human subjects for review and approval to each institution's Institutional Review Board (IRB), including explanations of how protected health information will be collected, used and disclosed in relation to the NCICB systems (45 CFR 46.103, *Assuring compliance with this policy -- research conducted or supported by any Federal Department or Agency*).

3.3 *Training*. All caBIG™ cancer centers and other institutions adopters seeking access to the NCICB systems must train all members of its workforce in the policies and procedures with respect to protected health information as necessary and appropriate for members of the workforce to carry out their functions involving access to and use of NCICB clinical data management systems. Training may be incorporated into current employee training programs (45 CFR 164.530(b)(1), *Standard: Training).*

3.4 The NCICB will follow comprehensive policies and procedures to prevent, detect, contain, and correct privacy violations related to the systems as required by the *Secure One HHS Information Security Program Policy* and *Information Security Program Handbook*. Consistent with this guidance, NCICB will:

3.4.1 Identify an NCI Information System Security Officer (Application ISSO) or equivalent official who will be responsible for implementing and enforcing NCI privacy policies consistent with applicable Federal law and this SOP.

3.4.2 Ensure that persons that receive or have access to human subjects' data using the NCICB systems are aware of the appropriate use of system resources and will adhere to Department-wide procedures for access, storage and transportation of all media containing sensitive information (as required by the *Secure One HHS Information Security Program Handbook*, Section 4.1.2, "Rules of Behavior", and the *Secure One HHS Information Security Program Handbook, Appendix G, "Rules of Behavior"* (see especially *"Media Control"*)).

3.4.4 Require cancer centers to document and report privacy breaches involving the use of the NCICB systems and respond to privacy breaches (as required by the *Secure One HHS Information Security Program Policy,* Section 4.9.1, "Security Incident and Violation Handling," and the *Secure One HHS Information Security Program Handbook,* Section 4.9.1, "Security Incident and Violation Handling."

3.4.5 Include in its response to privacy breaches involving the use of NCICB systems coordination with law enforcement authorities (as required by the *Secure One HHS Information Security Program Policy,* Section 4.9.1, "Security Incident and Violation Handling").

3.4.6 Require cancer centers to collect, maintain and access only the minimum amount of IIF necessary to conduct research using NCICB systems (as required by the *Secure One HHS Information Security Program Policy*, Section 4.1.6 ("Least Privilege") and the *Secure One HHS Information Security Program Handbook,* Section 4.1.6, "Least Privilege").

3.4.7 Conduct training, education and awareness of HHS privacy policies and procedures for all NCICB staff; and either conduct such training for cancer center staff that will access the NCICB systems, or seek assurances that the center has conducted such appropriate training (as required by the *Secure One HHS Information Security Program Policy,* Section 4.1.7 "Security Education and Awareness" and the *Secure One HHS Information Security Program Handbook,* Section 4.1.7 "Security Education and Awareness").

3.4.8 Monitor and document privacy compliance by cancer centers and other users of the NCICB systems, as required by the *Secure One HHS Information Security Program Policy,* Section 3.2, "Contractors and Outsourced Operations, and the Federal Information Security Management Act of 2002 (see especially the Office of Management and Budget Memorandum M-04-25, "Memorandum for Heads of Executive Departments and Agencies," August 23, 2004, requiring equivalent management oversight and compliance monitoring of contractor owned and operated systems as for government owned and operated information systems).

4. References /Regulations/Guidelines

Section	SOP Number	Title
4.1	N/A	Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
4.2	N/A	CDISC Glossary
4.3	N/A	SOP WG Glossary
4.4	N/A	Title 21 CFR Part 11
4.5	IT-001	SOP for Establishing and Maintaining the User Accounts
4.6	IT-002	SOP for Retiring User Accounts
4.7	CV-001	SOP for Complying with Title 21 CFR Part 11
4.8	AD-004	SOP for HIPAA Security Compliance
4.9	N/A	The E-Government Act of 2002, Section 208
4.10	N/A	The Privacy Act of 1974, as amended
4.11	N/A	Secure One HHS, Information Security Program Policy (December 15, 2004)

Section	SOP Number	Title
4.12	N/A	Secure One HHS, Information Security Program Handbook (December 15, 2004)
4.13	N/A	Title 45 CFR Part 46, Protection of Human Subjects
4.14	N/A	Title 45 CFR Part 164, Administrative Requirements
4.15	N/A	Title 42 CFR Part 164, Electronic Transactions

5. Roles & Responsibilities

Role	Responsibility
NCICB Applications Director	• Develop and implement policies and procedures for establishing that persons using caBIG™ systems maintained by NCICB to receive or have access to human subjects' data are aware of the acceptable use of that data. • Develop policy requiring cancer centers to have a written authorization from human subjects before using or disclosing their data using the caBIG™ environment. • Develop a policy requiring cancer centers to document and report privacy breaches involving the use of caBIG™ environment and responding to privacy breaches. • Develop and implement procedures for responding to breaches of privacy involving caBIG™ systems reported by cancer centers that includes coordination with law enforcement authorities. • Develop and implement a policy requiring cancer centers to collect, maintain and access only the minimum amount of information in identifiable form (IIF) necessary to conduct research using caBIG™ systems. • Develop procedures for conducting training, education and awareness of NCI privacy policies and procedures for all NCICB staff members. • Develop and implement procedures for monitoring and documenting privacy compliance by cancer centers and other users.
NCICB Information System Security Officer (Application ISSO)	• Develop, implement, and enforce policies and procedures for the protection of IIF.
Principal Investigator	• Obtain Institutional Review Board (IRB) approval for all research involving IIF. • Obtain authorization from human subjects that supply their data to the caBIG™ environment before disclosing it in any manner not previously described in the consent form described in section 3.1.2, subject to the exceptions laid out in the HIPAA Privacy Rule.

Role	Responsibility
	• Develop a privacy notice to human subjects as to how their data will be used within the caBIG™ environment and assure that it is provided to all human subjects.
Cancer Center Executives or their designees	• Assign roles and responsibilities for assuring that human subjects privacy is adequately protected to a workforce member or members.

6. Attachments

This SOP will be used in conjunction with the following attachments. These attachments must be used by all research sites conducting clinical trials under the caBIG™ Program and can be customized by individual research sites to accommodate format and content in accordance with local guidelines and/or requirements.

Title	Description
1) Procedure for Protecting Patient Privacy	This document provides the detailed steps to be followed in ensuring that access to caBIG™ systems supported by NCICB is in compliance with privacy rule requirements.